

**MINIMIZATION PROCEDURES USED BY THE NATIONAL  
SECURITY AGENCY IN CONNECTION WITH THE PRODUCTION  
OF CALL DETAIL RECORDS PURSUANT TO SECTION 501 OF THE  
FOREIGN INTELLIGENCE SURVEILLANCE ACT, AS AMENDED**

These National Security Agency (NSA) minimization procedures apply to the retention and dissemination of call detail records (CDRs), including non-publicly available information concerning unconsenting United States persons obtained from such CDRs, that are produced in accordance with Section 501 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act").

If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the National Security Division of the Department of Justice (NSD/DoJ), which will promptly notify the Foreign Intelligence Surveillance Court of such activity.

Except for the requirement that NSA promptly destroy any CDRs which are determined not to contain foreign intelligence information, nothing in these procedures shall restrict NSA's performance of lawful oversight functions of its personnel or systems, or the lawful oversight functions of the Congress of the United States, NSD/DoJ, Office of the Director of National Intelligence, or the applicable Offices of the Inspectors General.

For purposes of these procedures, the terms "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel will not disseminate CDRs, or information derived therefrom, outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of these procedures.

**A. Receipt and Initial Review.** Upon receiving CDRs from a Provider, NSA personnel will conduct an initial review of the CDRs. The review will be conducted through manual and/or automated inspection of the records to confirm that the CDRs are generally responsive to the Court's order, taking due account of the recordkeeping or other relevant practices of the producing party. This initial review will occur as soon as practicable following receipt of the CDRs and prior to the CDRs being made available for foreign intelligence analysis. NSA will promptly destroy CDRs produced that it determines are outside the scope of the Court's order.

**B. Storage of Call Detail Records.** NSA will process the collected CDRs to make the CDRs usable for intelligence analysis and store the records in repositories within secure networks under NSA's control. The CDRs will carry unique markings such that

software and other controls (including user authentication services) can restrict access to them. NSA will restrict access to the CDRs to authorized personnel who have received appropriate and adequate training with regard to these procedures.

**C. Sharing and Dissemination Procedures.** The CDRs may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all such NSA analysts first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. Appropriately and adequately trained NSA intelligence analysts may access, analyze and examine, the produced CDRs; may conduct research concerning the produced CDRs in NSA databases containing information acquired through other collection authorities such as E.O. 12333 and FISA, including available reports and collateral information (i.e., information to which NSA has access but did not originate, such as reports from other agencies and publicly available information); and may conduct technical analysis of the produced CDRs.

NSA will apply the minimization and dissemination requirements and procedures set forth below to information from the CDRs, in any form, before the information is disseminated outside of NSA in any form. A United States person means a United States person as defined in the Act. A number for a United States location, that is associated with a United States area code, or that is being used from inside the United States will be

presumed to be used by a United States person unless there is reason to believe otherwise.

A number for a location outside the United States, that is associated with a country code and a National Destination Code (colloquially, an "area code") outside the United States will be presumed not to be used by a United States person unless there is reason to believe otherwise. Numbers that are not known or presumed to be used by a United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.

1. A dissemination based on CDRs of or concerning a U.S. person will be written so as to focus solely on the activities of foreign entities and persons and their agents. Except as provided below, foreign intelligence information concerning U.S. persons must be disseminated in a manner which does not identify the U.S. person. Generic or general terms or phrases must be substituted for the identity (e.g., "U.S. firm" for the specific name of a U.S. corporation or "U.S. person" for the specific name of a U.S. person).

2. A dissemination may include the identification of a U.S. person only if one of the following conditions is met and a determination is made by the appropriate approval authority that the recipient has a need for the identity for the performance of his official duties:

- a. The U.S. person has consented to the dissemination, or

- b. The information of or concerning the U.S. person is publically available, or
- c. The identity of the U.S. person is necessary to understand the foreign intelligence information or assess its importance, or
- d. The identity of the U.S. person is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.

3. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Global Capabilities Manager of the Office of Counterterrorism, the Deputy Global Capabilities Manager for Counterterrorism Mission Capabilities, the Deputy Global Capabilities Manager for Counterterrorism Analysis and Production, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, or the Senior Operations Officer of the National Security Operations Center must determine that the information identifying the U.S. person is foreign intelligence information related to international terrorism, or is necessary to understand foreign intelligence information related to international terrorism or assess its importance.

4. Notwithstanding the above requirements, NSA may share, as appropriate, relevant information from the CDRs, including U.S. person identifying information, with Executive Branch personnel in order to enable them to determine whether the information may be exculpatory or otherwise discoverable in legal proceedings. Notwithstanding the above requirements, NSA may also share, as appropriate, the results from intelligence analysis of the CDRs with the Providers for the limited purpose of obtaining from the Providers a second set of call detail records created and maintained by the Providers per Section 501 of the Act.

5. Notwithstanding the above requirements, CDRs which do not contain foreign intelligence information related to international terrorism but are reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. § 1861(h), Executive Order 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such CDRs may be retained by NSA for a reasonable period of time, not to exceed six months unless

extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original CDRs are required for law enforcement purposes.

**D. Retention of Call Detail Records.** NSA personnel will exercise reasonable judgment in determining whether CDRs produced pursuant to the Order sought in this application contain foreign intelligence information, and will promptly destroy any CDRs which are determined not to contain foreign intelligence information. All call detail records obtained pursuant to the Order sought in this application will be destroyed no later than five years (60 months) after their initial collection, except that NSA may retain any CDR (or information derived therefrom) that was the basis of an approved dissemination. Also, NSA may temporarily retain specific CDRs that would otherwise have to be destroyed if the Department of Justice advises NSA in writing that the records are subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. The specific records to be retained, and the particular litigation for which the records will be retained, shall be identified in writing by the Department of Justice. Personnel not working on the particular litigation matter shall not access the unminimized records preserved pursuant to a written preservation notice from the Department of Justice that would otherwise have been destroyed pursuant to these procedures. Other personnel shall only access the records being retained for litigation-

related reasons on a case-by-case basis after consultation with the Department of Justice. The Department of Justice shall notify NSA in writing once the records are no longer required to be preserved for such litigation matters, and then NSA shall promptly destroy the records as otherwise required by these procedures. Circumstances could arise requiring that records subject to other destruction/age off requirements be retained because they are subject to a preservation requirement. In such cases the Government will notify the Foreign Intelligence Surveillance Court and seek permission to retain the material as appropriate consistent with law. Depending on the nature, scope and complexity of a particular preservation obligation, in certain circumstances it may be technically infeasible to retain certain records. Should such circumstances arise, they will be brought to the attention of the court with jurisdiction over the underlying litigation matter for resolution.

**E. National Security Division/Department of Justice Oversight of NSA Activities.**

NSA and the NSD/DoJ shall conduct oversight of NSA's activities under this authority as outlined below.

1. NSA's Office of General Counsel (OGC) and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the CDRs receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, retention, analysis, and



dissemination of the CDRs. The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his or her access to the CDRs and/or relevant NSA system architecture. NSA shall maintain records of all such training, and OGC shall provide NSD/DoJ with copies of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

2. NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services).

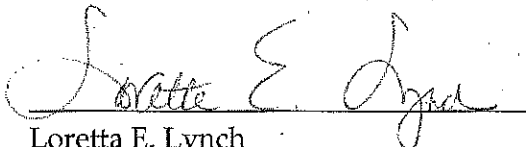
3. NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of these procedures. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

4. NSD/DoJ shall have access to all CDRs produced to NSA pursuant to Section 501 of FISA and other necessary information to facilitate minimization reviews and for all other lawful oversight purposes.

F. Approximately every thirty days, NSA shall file with the Court a report that includes a statement of the number of instances since the preceding report in which NSA has shared, in any form, information from the CDRs that contain United States person

information, in any form, with anyone outside NSA, other than Executive Branch personnel receiving such results in order to enable them to determine whether the information may be exculpatory or otherwise discoverable in legal proceedings and personnel of the Congress of the United States, NSD/DoJ, Office of the Director of National Intelligence, or the applicable Offices of the Inspectors General receiving such results in the performance of their lawful oversight functions. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

11/24/2015  
Date

  
Loretta E. Lynch  
Attorney General of the United States